Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	8262	traffic with monitoring	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L2	2629	security with association	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L3	64	L1 and L2	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L4	11299660	@ad<"20010129"	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L5	24	L4 and L3	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L6	15387	lucent.as.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L7	24	L5 not L6	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L8	24	L7	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57
L9	123	random with traffic with pattern$2	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:58
L10	0	8 and 9	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:58
L11	77	9 and 4	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:58
L12	8	1 and 11	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 16:11

L13	8	identif$6 same 9	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 16:12
S1	4961131	weight$3 amount$2 quantity priority level	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S2	3623424	traffic data packet communication transmission	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:39
S3	3081302	flow tunnel channel pathway	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:39
S4	531200	S2 with S3	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:39
S5	25237	quality near2 service	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:39
S6	28482	qos or S5	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:40
S7	63308	S1 with S4	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:40
S8	2399	ipsec	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:40
S9	1040466	time with period	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:40
S10	5811	S7 and S6	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41
S11	221	S8 and S10	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41

S12	11299659	@ad<"20010129"	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41
S13	48	S12 and S11	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41
S14	15385	lucent.as.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41
S15	47	S13 not S14	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/02 19:41
S16	8262	traffic with monitoring	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S17	2629	security with association	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S18	64	S16 and S17	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S19	11299660	@ad<"20010129"	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S20	24	S19 and S18	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S21	15387	lucent.as.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 13:45
S22	24	S20 not S21	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/11/03 15:57

Subscribe (Full Service)   Register (Limited Service, Free)   Login

Search: ◉ The ACM Digital Library   ○ The Guide

weighted traffic flow usage security association

THE ACM DIGITAL LIBRARY

📑 Feedback Report a problem Satisfaction survey

Terms used <u>weighted</u> <u>traffic</u> <u>flow</u> <u>usage</u> <u>security</u> <u>association</u>   Found **44,262** of **166,357**

Sort results by | relevance | ⬥ Save results to a Binder   Try an <u>Advanced Search</u>
Display results | expanded form | 🗐 Search Tips   Try this search in <u>The ACM Guide</u>
⬚ Open results in a new window

Results 1 - 20 of 200   Result page: **1** <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> <u>10</u>   <u>next</u>

Best 200 shown   Relevance scale ⬚⬚▨▩■

1 <u>Fast detection of communication patterns in distributed executions</u>   ■
Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**
Publisher: IBM Press
Full text available: 📄 <u>pdf(4.21 MB)</u>   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

> Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

2 <u>Protocol architectures: Lower than best effort: a design and implementation</u>   ▨
Ken Carlberg, Panos Gevros, Jon Crowcroft
April 2001 **ACM SIGCOMM Computer Communication Review**, Volume 31 Issue 2 supplement
Publisher: ACM Press
Full text available: 📄 <u>pdf(2.24 MB)</u>   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>

> In recent years, the Internet architecture has been augmented so that Better-than-Best-Effort (BBE) services, in the form of reserved resources for specific flows, can be provided by the network. To date, this has been realized through two different and sequentially developed efforts. The first is known as Integrated Services and focuses on specific bounds on bandwidth and/or delay for specific flows. The Differentiated Service model was later introduced, which presented a more aggregated and lo ...

3 <u>Packet classification in large ISPs: design and evaluation of decision tree classifiers</u>   ■
Edith Cohen, Carsten Lund
June 2005 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems SIGMETRICS '05**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: 📄 <u>pdf(195.66 KB)</u> Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

> Packet classification, although extensively studied, is an evolving problem. Growing and changing needs necessitate the use of larger filters with more complex rules. The increased complexity and size pose implementation challenges on current hardware solutions and drive the development of software classifiers, in particular, decision-tree based classifiers. Important performance measures for these classifiers are time and memory due to required high throughput and use of limited fast memory.We ...

Keywords: access control lists, decision trees, packet filtering, routing

4 Flow sampling under hard resource constraints

Nick Duffield, Carsten Lund, Mikkel Thorup

June 2004 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the joint international conference on Measurement and modeling of computer systems SIGMETRICS 2004/PERFORMANCE 2004**, Volume 32 Issue 1

Publisher: ACM Press

Full text available: pdf(246.84 KB)   Additional Information: full citation, abstract, references, citings, index terms

Many network management applications use as their data traffic volumes differentiated by attributes such as IP address or port number. IP flow records are commonly collected for this purpose: these enable determination of fine-grained usage of network resources. However, the increasingly large volumes of flow statistics incur concomitant costs in the resources of the measurement infrastructure. This motivates sampling of flow records.This paper addresses sampling strategy for flow records. Recen ...

Keywords: IP flows, sampling, variance reduction

5 New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice

Cristian Estan, George Varghese

August 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 3

Publisher: ACM Press

Full text available: pdf(1.03 MB)   Additional Information: full citation, abstract, references, citings, index terms, review

Accurate network traffic measurement is required for accounting, bandwidth provisioning and detecting DoS attacks. These applications see the traffic as a collection of flows they need to measure. As link speeds and the number of flows increase, keeping a counter for each flow is too expensive (using SRAM) or slow (using DRAM). The current state-of-the-art methods (Cisco's sampled NetFlow), which count periodically sampled packets are slow, inaccurate and resource-intensive. Previous work showed ...

Keywords: Network traffic measurement, identifying large flows, on-line algorithms, scalability, usage based accounting

6 Technical papers: DCAP: detecting misbehaving flows via collaborative aggregate policing

Chen-Nee Chuah, Lakshminarayanan Subramanian, Randy H. Katz

October 2003 **ACM SIGCOMM Computer Communication Review**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(281.15 KB)   Additional Information: full citation, abstract, references

This paper proposes a detection mechanism called *DCAP* for a network provider to monitor incoming traffic and identify misbehaving flows without having to keep per-flow accounting at any of its routers. Misbehaving flows refer to flows that exceed their stipulated bandwidth limit. Through collaborative aggregate policing at both ingress and egress nodes, DCAP is able to quickly narrow the search to a candidate group that contains the misbehaving flows, and eventually identify the individua ...

Keywords: flow-level accounting, misbehaving flow detection, traffic policing

7 Incentive-based modeling and inference of attacker intent, objectives, and strategies

Peng Liu, Wanyu Zang, Meng Yu

February 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume
8 Issue 1
Publisher: ACM Press
Full text available: pdf(963.16 KB)   Additional Information: full citation, abstract, references, index terms

Although the ability to model and infer attacker intent, objectives, and strategies (AIOS)
may dramatically advance the literature of risk assessment, harm prediction, and
predictive or proactive cyber defense, existing AIOS inference techniques are ad hoc and
system or application specific. In this paper, we present a general incentive-based
method to model AIOS and a game-theoretic approach to inferring AIOS. On one hand,
we found that the concept of incentives can unify a large variety of att ...

Keywords: Attacker intent and strategy modeling, attack strategy inference, game
theory

8   Resource management with hoses: point-to-cloud services for virtual private
networks
N. G. Duffield, Pawan Goyal, Albert Greenberg, Partho Mishra, K. K. Ramakrishnan, Jacobus
E. van der Merwe
October 2002 **IEEE/ACM Transactions on Networking (TON)**, Volume 10 Issue 5
Publisher: IEEE Press

Full text available: pdf(425.44 KB)   Additional Information: full citation, abstract, references, citings, index
terms

As IP technologies providing both tremendous capacity and the ability to establish
dynamic security associations between endpoints emerge, virtual private networks (VPNs)
are going through dramatic growth. The number of endpoints per VPN is growing and the
communication pattern between endpoints is becoming increasingly hard to predict.
Consequently, users are demanding dependable, dynamic connectivity between
endpoints, with the network expected to accommodate any traffic matrix, as long as
the ...

Keywords: point-to-cloud, point-to-multipoint, quality of service, service level
agreements

9   The transport layer: tutorial and survey
Sami Iren, Paul D. Amer, Phillip T. Conrad
December 1999 **ACM Computing Surveys (CSUR)**, Volume 31 Issue 4
Publisher: ACM Press

Full text available: pdf(261.78 KB)   Additional Information: full citation, abstract, references, citings, index
terms

Transport layer protocols provide for end-to-end communication between two or more
hosts. This paper presents a tutorial on transport layer concepts and terminology, and a
survey of transport layer services and protocols. The transport layer protocol TCP is used
as a reference point, and compared and contrasted with nineteen other protocols
designed over the past two decades. The service and protocol features of twelve of the
most important protocols are summarized in both text and tables.< ...

Keywords: TCP/IP networks, congestion control, flow control, transport protocol,
transport service

10   New directions in traffic measurement and accounting
Cristian Estan, George Varghese
August 2002 **ACM SIGCOMM Computer Communication Review , Proceedings of the
2002 conference on Applications, technologies, architectures, and
protocols for computer communications SIGCOMM '02**, Volume 32 Issue 4
Publisher: ACM Press

Full text available: 🔲 pdf(318.88 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

Accurate network traffic measurement is required for accounting, bandwidth provisioning and detecting DoS attacks. These applications see the traffic as a collection of flows they need to measure. As link speeds and the number of flows increase, keeping a counter for each flow is too expensive (using SRAM) or slow (using DRAM). The current state-of-the-art methods (Cisco's sampled NetFlow) which log periodically sampled packets are slow, inaccurate and resource-intensive. Previous work showed th ...

Keywords: identifying large flows, network traffic measurement, on-line algorithms, scalability, usage based accounting

11 <u>Data streaming algorithms for accurate and efficient measurement of traffic and flow matrices</u>
Qi (George) Zhao, Abhishek Kumar, Jia Wang, Jun (Jim) Xu
June 2005 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems SIGMETRICS '05**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: 🔲 pdf(299.15 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

The traffic volume between origin/destination (OD) pairs in a network, known as traffic matrix, is essential for efficient network provisioning and traffic engineering. Existing approaches of estimating the traffic matrix, based on statistical inference and/or packet sampling, usually cannot achieve very high estimation accuracy. In this work, we take a brand new approach in attacking this problem. We propose a novel data streaming algorithm that can process traffic stream at very high speed (e. ...

Keywords: data streaming, network measurement, sampling, statistical inference, traffic matrix

12 <u>HIDE: an infrastructure for efficiently protecting information leakage on the address bus</u>
Xiaotong Zhuang, Tao Zhang, Santosh Pande
October 2004 **ACM SIGPLAN Notices , ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the 11th international conference on Architectural support for programming languages and operating systems ASPLOS-XI**, Volume 39 , 38 , 32 Issue 11 , 5 , 5
Publisher: ACM Press
Full text available: 🔲 pdf(216.31 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

XOM-based secure processor has recently been introduced as a mechanism to provide copy and tamper resistant execution. XOM provides support for encryption/decryption and integrity checking. However, neither XOM nor any other current approach adequately addresses the problem of information leakage via the address bus. This paper shows that without address bus protection, the XOM model is severely crippled. Two realistic attacks are shown and experiments show that 70% of the code might be cracked ...

Keywords: address bus leakage protection, secure processor

13 <u>Identification and classification: Online identification of hierarchical heavy hitters: algorithms, evaluation, and applications</u>
Yin Zhang, Sumeet Singh, Subhabrata Sen, Nick Duffield, Carsten Lund
October 2004 **Proceedings of the 4th ACM SIGCOMM conference on Internet measurement**
Publisher: ACM Press

Full text available: ⬛ pdf(273.81 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

In traffic monitoring, accounting, and network anomaly detection, it is often important to be able to detect high-volume traffic clusters in near real-time. Such heavy-hitter traffic clusters are often hierarchical (<i>ie</i>, they may occur at different aggregation levels like ranges of IP addresses) and possibly multidimensional (<i>ie</i>, they may involve the combination of different IP header fields like IP addresses, port numbers, and protocol). Without prior knowledge a ...

Keywords: change detection, data stream computation, hierarchical heavy hitters, network anomaly detection, packet classification

14 Media synchronization and QoS packet scheduling algorithms for wireless systems   ⬛
Azzedine Boukerche, Harold Owens
February 2005 **Mobile Networks and Applications**, Volume 10 Issue 1-2
Publisher: Kluwer Academic Publishers
Full text available: ⬛ pdf(579.10 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

Wireless multimedia synchronization is concerned with distributed multimedia packets such as video, audio, text and graphics being played-out onto the mobile clients via a base station (BS) that services the mobile client with the multimedia packets. Our focus is on improving the Quality of Service (QoS) of the mobile client's on-time-arrival of distributed multimedia packets through network multimedia synchronization. We describe a media synchronization scheme for wireless networks, ...

Keywords: distributed algorithms, media synchronization, mobile multimedia, packet scheduling algorithm, quality of service (QoS), wireless communications

15 A flexible model for resource management in virtual private networks   ⬛
◈ N. G. Duffield, Pawan Goyal, Albert Greenberg, Partho Mishra, K. K. Ramakrishnan, Jacobus E. van der Merive
August 1999 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '99**, Volume 29 Issue 4
Publisher: ACM Press

Full text available: ⬛ pdf(1.67 MB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

As IP technologies providing both tremendous capacity and the ability to establish dynamic secure associations between endpoints emerge, Virtual Private Networks (VPNs) are going through dramatic growth. The number of endpoints per VPN is growing and the communication pattern between endpoints is becoming increasingly hard to forecast. Consequently, users are demanding dependable, dynamic connectivity between endpoints, with the network expected to accommodate any traffic matrix, as long as the ...

16 Service infastructure and network management: Architecture and techniques for   ⬛
◈ diagnosing faults in IEEE 802.11 infrastructure networks
Atul Adya, Paramvir Bahl, Ranveer Chandra, Lili Qiu
September 2004 **Proceedings of the 10th annual international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: ⬛ pdf(303.82 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

The wide-scale deployment of IEEE 802.11 wireless networks has generated significant challenges for Information Technology (IT) departments in corporations. Users frequently complain about connectivity and performance problems, and network administrators are expected to diagnose these problems while managing corporate security and coverage. Their task is particularly difficult due to the unreliable nature of the wireless medium and

a lack of intelligent diagnostic tools for determining the cause ...

Keywords: IEEE 802.11, disconnected clients, fault detection, fault diagnosis, infrastructure wireless networks, rogue APs

17 Robustness: Defensive programming: using an annotation toolkit to build DoS-resistant software
Xiaohu Qie, Ruoming Pang, Larry Peterson
December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Publisher: ACM Press
Full text available: pdf(2.13 MB)   Additional Information: full citation, abstract, references

This paper describes a toolkit to help improve the robustness of code against DoS attacks. We observe that when developing software, programmers primarily focus on functionality. Protecting code from attacks is often considered the responsibility of the OS, firewalls and intrusion detection systems. As a result, many DoS vulnerabilities are not discovered until the system is attacked and the damage is done. Instead of reacting to attacks after the fact, this paper argues that a better solution i ...

18 Virtual-topology adaptation for WDM mesh networks under dynamic traffic
Aysegül Gençata, Biswanath Mukherjee
April 2003 **IEEE/ACM Transactions on Networking (TON)**, Volume 11 Issue 2
Publisher: IEEE Press
Full text available: pdf(585.44 KB)   Additional Information: full citation, abstract, references, index terms

We present a new approach to the virtual-topology reconfiguration problem for a wavelength-division-multiplexing-based optical wide-area mesh network under dynamic traffic demand. By utilizing the measured Internet backbone traffic characteristics, we propose an adaptation mechanism to follow the changes in traffic without *a priori* knowledge of the future traffic pattern. Our work differs from most previous studies on this subject which redesign the virtual topology according to an expect ...

Keywords: WDM, dynamic traffic, mesh network, mixed-integer linear program (MILP), optical network, virtual-topology reconfiguration

19 FIRE: flexible Intra-AS routing environment
Craig Partridge, Alex C. Snoeren, W. Timothy Strayer, Beverly Schwartz, Matthew Condell, Isidro Castiñeyra
August 2000 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication SIGCOMM '00**, Volume 30 Issue 4
Publisher: ACM Press
Full text available: pdf(107.75 KB)   Additional Information: full citation, abstract, references, index terms

Current routing protocols are monolithic, specifying the algorithm used to construct forwarding tables, the metric used by the algorithm (generally some form of hop-count), and the protocol used to distribute these metrics as an integrated package. The Flexible Intra-AS Routing Environment (FIRE) is a link-state, intra-domain routing protocol that decouples these components. FIRE supports run-time-pro- grammable algorithms and metrics over a secure link-state distribution protocol. By allow ...

20 ACCEL-RATE: a faster mechanism for memory efficient per-flow traffic estimation
Fang Hao, Murali Kodialam, T. V. Lakshman
June 2004 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the joint international conference on Measurement and modeling of computer systems SIGMETRICS 2004/PERFORMANCE 2004**, Volume 32 Issue 1
Publisher: ACM Press
Full text available: pdf(252.00 KB)   Additional Information: full citation, abstract, references, index terms

Per-flow network traffic measurement is an important component of network traffic management, network performance assessment, and detection of anomalous network events such as incipient DoS attacks. In [1], the authors developed a mechanism called RATE where the focus was on developing a memory efficient scheme for estimating per-flow traffic rates to a specified level of accuracy. The time taken by RATE to estimate the per-flow rates is a function of the specified estimation accuracy and this t ...

Results 1 - 20 of 200   Result page: **1**   2   3   4   5   6   7   8   9   10   next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player

P⊘RTAL

USPTO

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **ipsec security association**   Found **12,634** of **166,357**

Sort results by   relevance ▾   ✦ Save results to a Binder   Try an Advanced Search
                                                                                    Try this search in The ACM Guide
Display results   expanded form ▾   ▣ Search Tips

                                              ▦ Open results in a new window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown   Relevance scale ▯▭▬◼◼

1   Trust management for IPsec   ◼

May 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 2

Publisher: ACM Press

Full text available: 🗎 pdf(321.98 KB)   Additional Information: full citation, abstract, references, citings, index terms, review

IPsec is the standard suite of protocols for network-layer confidentiality and authentication of Internet traffic. The IPsec protocols, however, do not address the policies for how protected traffic should be handled at security end points. This article introduces an efficient policy management scheme for IPsec, based on the principles of trust management. A compliance check is added to the IPsec architecture that tests packet filters proposed when new security associations are created for confo ...

Keywords: Credentials, IPsec, KeyNote, network security, policy, trust management

2   The DGSA: unmet information security challenges for operating system designers   ◼

Edward A. Feustel, Terry Mayfield
January 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 1

Publisher: ACM Press

Full text available: 🗎 pdf(1.48 MB)   Additional Information: full citation, abstract, citings, index terms

The Department of Defense (DoD) Goal Security Architecture (DGSA) introduces a broader view of information security from that previously held by the Department, one which has much more in common with the requirements of an inter-networked commercial view of information security. The purpose of this paper is to introduce designers of operating systems to the most important aspects of the DGSA conceptual framework in order to open discussions on both the suitability of the framework and the feasib ...

3   Formal prototyping in early stages of protocol design   ◼

Alwyn Goodloe, Carl A. Gunter, Mark-Oliver Stehr
January 2005 **Proceedings of the 2005 workshop on Issues in the theory of security**

Publisher: ACM Press

Full text available: 🗎 pdf(530.03 KB)   Additional Information: full citation, abstract, references

Network protocol design is usually an informal process where debugging is based on successive iterations of a prototype implementation. The feedback provided by a prototype can be indispensable since the requirements are often incomplete at the start. A draw-back of this technique is that errors in protocols can be notoriously difficult to detect by testing alone. Applying formal methods such as theorem proving can greatly increase one's confidence that the protocol is correct. However, formal m ...

4 Securing wireless applications: On securely enabling intermediary-based services and performance enhancements for wireless mobile users

Sneha Kasera, Semyon Mizikovsky, Ganapathy S. Sundaram, Thomas Y. C. Woo
September 2003 **Proceedings of the 2003 ACM workshop on Wireless security**
Publisher: ACM Press
Full text available: pdf(310.72 KB)   Additional Information: full citation, abstract, references, index terms

Intermediary-based services and performance optimizations are increasingly being considered, by network service providers, with a view towards offering value-added services and improving the user experience of wireless mobile clients at reduced costs. However, in the presence of an end-to-end security mechanism such as IPsec, it is impossible to offer such services without fully compromising end-to-end security. We propose a new architecture to enable intermediary-based services for wireless mob ...

Keywords: IPsec, end-to-end security, intermediary, mobile, performance, wireless

5 An adaptive cryptographic engine for internet protocol security architectures

Andreas Dandalis, Viktor K. Prasanna
July 2004 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**,
Volume 9 Issue 3
Publisher: ACM Press
Full text available: pdf(264.87 KB)   Additional Information: full citation, abstract, references, index terms

Architectures that implement the Internet Protocol Security (IPSec) standard have to meet the enormous computing demands of cryptographic algorithms. In addition, IPSec architectures have to be flexible enough to adapt to diverse security parameters. This article proposes an FPGA-based Adaptive Cryptographic Engine (ACE) for IPSec architectures. By taking advantage of FPGA technology, ACE can adapt to diverse security parameters on the fly while providing superior performance compared with softw ...

Keywords: AES, Adaptive computing, IPSec, configurable, cryptography, high performance, performance tradeoffs, reconfigurable components, reconfigurable computing, reconfigurable systems

6 Mobile IP and the IETF

Charles E. Perkins
April 2002 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 6
Issue 2
Publisher: ACM Press
Full text available: pdf(59.51 KB)   Additional Information: full citation, index terms

7 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB)   Additional Information: full citation, references, citings, index terms

8 Miscellany: Quantum cryptography in practice

Chip Elliott, David Pearson, Gregory Troxel
August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications**
Publisher: ACM Press

Full text available: pdf(809.93 KB)   Additional Information: full citation, abstract, references, index terms

BBN, Harvard, and Boston University are building the DARPA Quantum Network, the world's first network that delivers end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks. The first network link has been up and steadily operational in our laboratory since December 2002. It provides a Virtual Private Network between private enclaves, with user traffic protected by a weak-coherent implementation of quantum cryptogra ...

Keywords: IPsec, cryptographic protocols, error correction, key agreement protocols, privacy amplification, quantum cryptography, quantum key distribution, secure networks

9 Implementing a distributed firewall

Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, Jonathan M. Smith
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(309.36 KB)   Additional Information: full citation, references, citings, index terms

Keywords: IKE, IP, IPsec, KeyNote, OpenBSD, access control, credentials, distributed, firewalls, network security, trust management

10 A public-key based secure mobile IP

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra
September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: pdf(1.95 MB)   Additional Information: full citation, references, citings

11 Mobility, roaming, and handoff: Secure universal mobility for wireless internet

Ashutosh Dutta, Tao Zhang, Sunil Madhani, Kenichi Taniuchi, Kensaku Fujimoto, Yasuhiro Katsube, Yoshihiro Ohba, Henning Schulzrinne
October 2004 **Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots**
Publisher: ACM Press
Full text available: pdf(1.10 MB)   Additional Information: full citation, abstract, references, index terms

The advent of the mobile wireless Internet has created the need for seamless and secure communication over heterogeneous access networks such as IEEE 802.11, WCDMA, cdma2000, and GPRS. An enterprise user desires to be reachable while outside one's enterprise networks and requires minimum interruption while ensuring that the signaling and data traffic is not compromised during one's movement within the enterprise and between enterprise and external networks. We describe the design, implementat ...

Keywords: 802.11, handoff, hot spot, mobile IP, mobility, security

12 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(118.52 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

13 <u>Best papers from WMASH 2004: Secure universal mobility for wireless Internet</u>
Ashutosh Dutta, Tao Zhang, Sunil Madhani, Kenichi Taniuchi, Kensaku Fujimoto, Yasuhiro Katsube, Yoshihiro Ohba, Henning Schulzrinne
July 2005 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 9 Issue 3
Publisher: ACM Press
Full text available: pdf(1.47 MB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>

The advent of the mobile wireless Internet has created the need for seamless and secure communication over heterogeneous access networks such as IEEE 802,11, WCDMA, cdma2000, and GPRS. An enterprise user desires to be reachable while outside one's enterprise networks and requires minimum interruption while ensuring that the signaling and data traffic is not compromised during one's movement within the enterprise and between enterprise and external networks. We describe the design, implementation ...

14 <u>Papers: Child-proof authentication for MIPv6 (CAM)</u>
Greg O'Shea, Michael Roe
April 2001 **ACM SIGCOMM Computer Communication Review**, Volume 31 Issue 2
Publisher: ACM Press
Full text available: pdf(464.24 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

We present a unilateral authentication protocol for protecting IPv6 networks against abuse of mobile IPv6 primitives. A mobile node uses a partial hash of its public key for its IPv6 address. Our protocol integrates distribution of public keys and protects against falsification of network addresses. Our protocol is easy to implement, economic to deploy and lightweight in use. It is intended to enable experimentation with (mobile) IPv6 before the transition to a comprehensive IPSEC infrastructure ...

Keywords: IPNG, IPv6, Mobility, mobile communications

15 <u>Military applications: Security issues in high level architecture based distributed simulation</u>
Asa Elkins, Jeffery W. Wilson, Denis Gracanin
December 2001 **Proceedings of the 33nd conference on Winter simulation**
Publisher: IEEE Computer Society
Full text available: pdf(262.26 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

The United States Department of Defense (DoD) has, over the past several years, emphasized the need to employ simulation based acquisition (SBA) in engineering and development. Distributed simulation introduces an information assurance challenge and details of a simulation must be guarded from unauthorized access. The High Level Architecture (HLA) and its Run-Time Interface (RTI) do not define support of mandatory access controls (MACs) or discretionary access controls (DACs) required to provide ...

16 <u>Secure group communications: Group security association (GSA) management in IP multicast</u>
Thomas Hardjono, Mark Baugher, Hugh Harney

June 2001 **Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge**

Additional Information: full citation, abstract, references, index terms

This work describes the Group Security Association (GSA) Management model and protocol as developed in the Secure Multicast Group (SMUG) in the IETF. The background reasoning from the Internet Key Exchange (IKE) protocol perspective is explained, together with the notion of Security Associations (SA) in the unicast cast. This serves as a basis for requirements for Group SA for multicast. Finally, the definition and construction of a GSA is described.

Keywords: IETF, IKE, IPSEC, group security, key management, multicast security, security associations

17 Internet security: firewalls and beyond
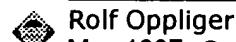
Rolf Oppliger

May 1997 **Communications of the ACM**, Volume 40 Issue 5

Publisher: ACM Press

Full text available: pdf(339.15 KB)   Additional Information: full citation, references, citings, index terms, review

18 Focus on the Asanté FriendlyNet VR2004 series VPN security router

Gilbert Held

November 2003 **International Journal of Network Management**, Volume 13 Issue 6

Publisher: John Wiley & Sons, Inc.

Full text available: pdf(233.16 KB)   Additional Information: full citation, index terms

19 Design of a high-performance ATM firewall

Jun Xu, Mukesh Singhal

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Publisher: ACM Press

Full text available: pdf(143.19 KB)   Additional Information: full citation, abstract, references, index terms

A router-based packet-filtering firewall is an effective way of protecting an enterprise network from unauthorized access. However, it will not work efficiently in an ATM network because it requires the termination of end-to-end ATM connections at a packet-filtering router, which incurs huge overhead of SAR (Segmentation and Reassembly). Very few approaches to this problem have been proposed in the literature, and none is completely satisfactory. In this paper we present the hardware desig ...

Keywords: TCP/IP, asynchronous transfer mode, firewall, packet filtering, switch architecture

20 Ubiquitous computing/security: Securing nomads: the case for quarantine, examination, and decontamination

Kevin Eustice, Leonard Kleinrock, Shane Markstrum, Gerald Popek, V. Ramakrishna, Peter Reiher

August 2003 **Proceedings of the 2003 workshop on New security paradigms**

Publisher: ACM Press

Full text available: pdf(693.40 KB)   Additional Information: full citation, abstract, references, index terms

The rapid growth and increasing pervasiveness of wireless networks raises serious security concerns. Client devices will migrate between numerous diverse wireless environments, bringing with them software vulnerabilities and possibly malicious code.

Techniques are needed to protect wireless client devices and the next generation wireless infrastructure. We propose QED, a new security model for wireless networks that enables wireless environments to quarantine devices and then analyze and potenti ...

Keywords: decontamination, examination, mobile computing, nomadic computing, pervasive computing, quarantine, security, ubiquitous computing, wireless, worm

Results 1 - 20 of 200   Result page: **1**   2   3   4   5   6   7   8   9   10   next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player